AMENDMENTS TO THE CLAIMS

Please cancel claim 1 and replace it with claim 11:

1. (Cancelled)

2. (Currently Amended) The method as defined ~~claimed~~ in claim 1, wherein the sequence number ~~(12, 22a, 22a')~~ is transmitted together with the signing key [[(14)]] from the control center to the sender [[(20)]], and is transmitted from the sender [[(20)]] via the data set ~~(22, 22')~~ to the receiver.

3. (Currently Amended) The method as defined ~~claimed~~ in claim 1, wherein the sequence numbers are used to produce signing keys in the control center and corresponding checking keys in the receiver. ~~number (12) is produced by a generator in synchronism with the number of signing and check keys used in the control center (10) and in the receiver.~~

4. (Currently Amended) The method as defined ~~claimed~~ in claim 1, wherein the sequence numbers are used to produce signing keys used in the control center and corresponding check keys are used in the receiver wherein the sequence number is transmitted via the data set to the receiver. ~~sequence number (12) is produced by a generator in synchronism with the number of signing and check keys used in the control center (10) and in the sender, and is transmitted via the data set (22, 22') to the receiver.~~

5. (Previously Presented) The method as defined ~~claimed~~ in claim 1, wherein the sequence number is produced by a pseudo-random number generator.

6. (Previously Presented) The method as defined ~~claimed~~ in claim 1, wherein the encryption of the sequence number by means of the main key is used as the one-time encryption.

7. (Previously Presented) The method as defined ~~claimed~~ in claim 1, wherein the control center [[(10)]] produces a number of signing keys [[(14)]] in advance, and transmits them to the sender [[(30)]], either separately or ~~possibly~~ together with the associated sequence numbers [[(12)]].

8. (Previously Presented) The method as defined ~~claimed~~ in claim 1, wherein the receiver [[(30)]] maintains a list of already used sequence numbers, and rejects already used sequence numbers.

9. (Currently Amended) A device for signing a message ~~(22, 22')~~ which is sent from a sender [[(20)]] to a receiver ~~(30), having the following features~~ comprising:

- a control center [[(10)]] having a first memory and the receiver [[(30)]] having a second memory ~~have a first and a second memory~~ for a secret, common main key ~~(11, 11')~~;
- in the control center [[(10)]], one input of a first one-time encrypter [[(13) is]] being connected to the first ~~protected~~ memory [[(11)]] of the control center, and another input [[is]] being connected to a generator [[(12)]] for a sequence number,
- an [[the]] output of the one-time encrypter ~~(13) is~~ being connected to the sender [[(20)]] via a transport medium,
- a signature generator ~~(24) is~~ provided in the sender, and having [[its]] inputs [[are]] connected to the output of the one-time encrypter and to the message ~~(21, 22b)~~ to be signed,
- [[the]] an output of the signature generator ~~(24) is~~ being connected to a device which assembles at least the signature [[(22c)]] and the message [[(22b)]] to form a data message block [[(22)]] and whose output is connected to the receiver [[(30)]] via a transport medium,
- a signature checker ~~(22') is~~ provided in the receiver [[, whose]] having inputs[[are]] connected ~~firstly~~ to the message ~~(22b')~~ and to the signature [[(22c)]] of the data message block [[(22')]] which has arrived via the transport medium, and wherein
- ~~and secondly~~ the inputs of the signature checker are further connected to [[the]] an output of a second one-time encrypter [[(13')]], whose inputs are connected ~~firstly~~ to the second memory [[(11')]] of the receiver for the secret main key and to a means for providing a sequence number ~~(22a')~~.

10. (Previously Presented) The device as defined ~~claimed~~ in claim 9, wherein [[a]] the generator to produce a sequence number [[using]] uses a deterministic method to produce ~~produces~~ one or more sequence numbers ~~corresponding~~ that correspond to the same number of ~~checks~~ check keys.

11. (New) A method for signing a message from a sender and for checking a signature at a receiver, the method comprising the steps of:

providing a control center, a sender and a receiver wherein the control center and the receiver share an undiscoverable main key;

causing the control center to produce one or more sequence numbers;

using one of the sequence numbers and the common main key to create a signing key by means of a one-time encryption;

providing the signing key and the sequence number to the sender via a secure transmission;

the sender using the signing key to form a signature for a message and sending the message to the receiver via a data set containing at least the message and the signature;

determining the sequence number from the received data set;

passing the sequence number through a one-time encryption to produce a check key; and

using the check key to verify the signature on the message.